CLASSIFICATION OF THE DCID

Unless there are compelling reasons to the contrary, we believe the draft DCID should be unclassified. The following reasons pertain:

1. The most important reason for unclassified publication of the DCID is to make known to potential suppliers of automated systems and related services (e.g., software security packages) the security requirements and capabilities we need to have provided in off-the-shelf systems. The whole thrust of the DoD Computer Security Initiative Program since its inception in 1978 has been based upon the clear reality that DoD simply cannot afford to build and maintain specialized secure systems. Rather, we must to the utmost encourage industry to develop, build and maintain such systems. Subparagraph II.7., "Systems Acquisition," of the DCID specifically relates to this point.

2. Our computer security policy issuances, DoD Directive 5200.28 and DoD Manual 5200.28-M, largely parallel and are consistent with past issuances of DCID 1/16, and they have been unclassified for over 10 years, with no known adverse effects. Similarly, our computer security policies for contractor ADP systems have been disseminated on an unclassified basis for years.

3. The draft DCID has been handled as unclassified throughout its many versions.

If an unclassified version is deemed feasible, we recommend that it be marked as FOUO and exempted from public release under exemptions 2 & 3 to the Freedom of Information Act.

If the foregoing is not feasible, then we recommend that a sanitized version of DCID 1/16 be developed to disseminate the substance of the DCID outside the Intelligence Community as was previously proposed some years ago (i.e., Chairman, SECOM, memorandum IRSEC-PR/54, December 5, 1973, subject: " Sanitized Version of DCID No. 1/16 for USIB Contractors and Non-USIB Government Agencies").

On file OSD release instructions apply.